REMARKS

The Office Action mailed September 5, 2003 has been received and reviewed. Claims 23-56 are pending and are rejected. Claims 23-56 are cancelled. Claims 57-89 are added. Support for the new claims is found in paragraphs [0018] through [0025] as originally filed in the specification, and elsewhere in the specification and drawings. For the reasons stated herein, the Applicants submit that the claims are in condition for allowance.

Objection To Drawings Under 37 C.F.R. § 1.83(a)

The drawings are objected to for failing to show elements of claims 50, 51 and 53-56. The objection is rendered moot by cancellation of the claims. The Applicants note, however, that all elements of new claims 57-89 are shown in the drawings.

Rejection Of Claims 23-56 Under 35 U.S.C. § 112, First Paragraph

Claims 23-56 are rejected under 35 U.S.C. § 112, first paragraph as containing subject matter which was not described in the specification in a manner to convey to one of skill in the art that the inventors had possession of the claimed invention at the time the application was filed. The rejection is rendered moot by the cancellation of claims 23-56, but the Applicants submit that with respect to the elements of newly added claims 57-89, the claims are fully supported by the specification as originally filed.

Rejection Of Claims 40, 44, 46 And 47 Under 35 U.S.C. § 112, Second Paragraph

Claims 40, 44, 46 and 47 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite. The rejection is moot by cancellation of the claims.

Rejection Of Claims 23, 25-35, 38 41, 42, 45-49 and 53 Under 35 U.S.C. § 103(a)

Claims 23, 25-35, 38, 41, 42, 45-49 and 53 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bishop in view of Badger. The rejection is rendered moot by cancellation of the claims. However, the Applicants submit that newly added claims 57-89 are neither anticipated nor rendered obvious by Bishop since Bishop discloses a vehicle with an audio-warning device that comprises the deactivation of several electronic operating components, such as the ignition and door lock, but that such deactivation is reversible by electronically bridging the relay of the system, or by other means. Claims 57-89 require irreversible deactivation of the electronic operating components of the object. While Badger discloses use of a satellite to send a radio signal, Badger too discloses a reversible disabling system (See column 2, lines 59-62). Therefore, neither Bishop nor Badger, alone or in combination, teach or suggest that which is claimed and, to the contrary, the references teach away from what is claimed.

Rejection Of Claim 24 Under 35 U.S.C. § 103(a)

Claim 24 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bishop and Badger in view of Besharat. The rejection is made moot by cancellation of the claims. However, the Applicants reiterate that neither Bishop nor Badger, either alone or in combination, anticipates or renders obvious that which is claimed, and that the two references, in fact, teach away from what is claimed. Additionally, Besharat does not teach a signaling system that requires the receiving component to be brought into radio contact within a predetermined interval of time as required in new claim 59.

Rejection Of Claims 36, 37, 39 and 40 Under 35 U.S.C. § 103(a)

Claims 36, 37, 39 and 40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bishop and Badger in view of Szarka. The Examiner states that in analogous art, Szarka shows a vehicle disablement system that uses an interrogation-response communication to determine location and authenticity of the vehicle to

properly disable the vehicle and that it would have been obvious to provide such an improved security in the disablement system. Again, the rejection is rendered moot by cancellation of the claims. However, as stated previously, neither Bishop nor Badger, either alone or in combination, anticipates or renders obvious that which is claimed. Additionally, in reference to current claims 64 through 71, Szarka, like Bishop and Badger, discloses a reversible disablement system contrary to that which is claimed. Moreover, Szarka fails to provide any disclosure of the use of unique identifying numbers in a signal to verify the integrity of the disablement transmission. To the contrary, Szarka teaches a system having a plurality of remote transmitters, any one of which is operable and able to disable the equipment. The teaching of Szarka is, therefore, antithetical to the present invention. The claims are, therefore, neither anticipated nor obviated by Szarka alone or in combination with Bishop and Badger.

Rejection Of Claims 50, 52, 54 and 55 Under 35 U.S.C. § 103(a)

Claims 50, 52, 54 and 55 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bishop and Badger in view of Kaish. The Examiner states that in analogous art, Kaish shows a disabling device that renders electronic appliances inoperable to dissuade theft. The Examiner takes official notice that the claimed elements are common well known electronic appliances and it would have been obvious to modify the disabling system to render the electronic keys and smart cards inoperable to deter theft. The rejection is rendered moot with cancellation of the claims. However, the new claims are not anticipated or obviate by either Bishop or Badger for the reasons stated previously, and Kaish does not teach or suggest that which is claimed.

Rejection Of Claims 51 and 56 Under 35 U.S.C. § 103(a)

Claims 51 and 56 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bishop and Badger in view of Rohrbach. The Examiner states that in analogous

art, Rohrbach shows a disabling device that renders portable telephone appliances inoperable to prevent theft and that it would have been obvious to use a modified disabling system to render a portable telephone appliance inoperable to deter theft. The rejection is rendered moot by the cancellation of the claims, but the Applicants reiterate that the present claims are neither anticipated nor obviated by Bishop and Badger for the reasons previously stated, notwithstanding any teaching of Rohrbach.

CONCLUSION

In view of the arguments presented herein, the Applicants submit that claims 57-89 present patentable subject matter. Reconsideration and allowance are requested.

Respectfully submitted,

Julie K. Morriss
Registration No. 33,263
Attorney for Applicants
MORRISS O'BRYANT COMPAGNI, P.C.
136 South Main Street, Suite 700
Salt Lake City, Utah 84101
Telephone: (801) 478-0071
Facsimile: (801) 478-0076

Date: December 4, 2003

Attachments: Substitute Specification - Marked up copy
Substitute Specification - Clean form
Replacement Sheets of Drawings - FIGS. 1-3

[[(]]Safety Device for Overall Protection of Objects with Electronic Components[(])]

~~Description~~

~~Felix Huber, Ernst Messerschmid, and Wolfgang Schäfer~~

[0001] Cross-Reference to Related Applications: The present application is the U.S. National phase of PCT/EP99/01082, filed February 19, 1999, which claims priority to German Patent Application No. 1980766.7 filed February 20, 1998.

BACKGROUND OF THE INVENTION

[0002] Field of the Invention: This invention relates to devices and methods for protecting objects with electronic components.

[0003] Description of Related Art: It is known that electrical components can be controlled remotely by radio signals. A typical application is an electronic alarm system and/or drive lock of a vehicle, which the user activates or deactivates with a transmitter. In this case, it does not matter whether the transmitter radiates directly (e.g., through infrared transmission) or public radio serves or telephone networks are connected in between. However, if anti-theft protection is implemented in such a way that the object to be protected can be reactivated by disconnecting or bridging the protection device, then the protection is practically useless.

[0004] Typical characteristics and problems of such protection will be explained with the example of a vehicle. In principle, such a protection can be used for all objects with an electronic component. This can include, among other things: radio telephone ("handies"), (Euro-)Check and money cards, credit cards, telephone cards, keys for electronic lock systems, mobile electronic devices such as cassette recorders, CD players, clocks, computers, etc.

[0005] It is known that vehicles with mechanical and/or electric anti-theft protection devices can be reactivated by disassembly or bridging. This applies especially to expensive vehicles, where the entire vehicle can simply be transported by organized bands and worked on at a safe place. It is also known that vehicles with an electronic drive lock, often part of the motor control, can only be reactivated at great expense and with special knowledge. Often, reactivation is possible only with an original key and/or by involving a contract workshop.

[0006] Since with a stolen original key the vehicle can be made ready to drive immediately, a change from simple vehicle theft to theft by personal threat is being observed. Deactivation by a small hand transmitter a few hundred meters away could be conceived, but this brings the danger that the victim himself is placed in danger if the culprit becomes aware of the existence of the transmitter.

[0007] In order to make certain that the proper owner is protected, concepts have already been thought up in which the vehicle regularly receives radio signals for release of the electronics and

is deactivated if these signals are absent. In a stolen vehicle, these signals can then be turned [of] off intentionally, so that the vehicle can no longer be operated. This, however, has the disadvantage that when a radio gap appears, which is repeatedly the case with mobile telephones, further driving is no longer possible. In addition, a gapless coverage of the radio range must also be provided in other countries, since a temporary turning off of the protection during a stay abroad again makes the protection absurd. Such protection, however, means a strong restriction for legal users and therefore cannot be put on the market.

[0008] It is also known that there are devices in which a circuit in the vehicle can be activated that deactivates the ignition electronics. Such systems can be realized through a telephone connection that the user activates by dialing a particular number assigned to the vehicle receiver. Here too, global accessibility of the vehicle must be considered. These systems, however, could be circumvented by removing the receiver from the vehicle or by correspondingly shielding it from receiving signals, so that a blocking of the ignition electronics no longer occurs.

[0009] For universal protection, therefore, the system must be constructed in such a way that reactivation cannot take place through the user himself, for otherwise the information necessary for this could be obtained by force. Also, deactivation of the system must be able to take place at any time after the theft. This deactivation can also be performed by third parties, so that a threat to or even killing of the owner does not help. For a thief, therefore, stealing such an object has no value, since within a few hours it will no longer have its desired functionality.

~~**Method of operation.**~~

BRIEF SUMMARY OF THE INVENTION

[0010] The present invention avoids the disadvantages mentioned above by irreversibly deactivating and/or erasing at least one of the anti-theft components, and/or information within at least one of the anti-theft components, of a stolen object that are essential for use or operation of the stolen object, such as, for example, a vehicle, mobile phone or credit card. In the case of a stolen vehicle, for example, those anti-theft components may include, for example, the motor electronics, the steering column lock, the door lock 8 and/or the ignition key.

[0011] In order to achieve worldwide protection, a radio signal may preferably be radiated by a low-orbiting satellite and/or a space station with an on-board transmitter that is capable of transmitting a signal over the face of the earth to cover the inhabited parts of the earth. If an object, such as a vehicle, is stolen, a radio signal may be transmitted from space to deactivate, for example, one or more of the anti-theft components in the vehicle. This may be accomplished, in one method, by transmitting a signal from an emergency center to the satellite to trigger the transmission of a radio signal for deactivation of the components of the vehicle.

[0012] Alternatively, the radio signal may erase indispensable important information which enables the stolen object to be used or operated. Electronic components associated with the stolen object recognize that the important information has been erased, thereby depriving the stolen object of the necessary information needed to operate properly. These and other features of the invention are described further below.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0013] In the drawings, which illustrate what is currently considered to be the best mode for carrying out the present invention:

[0014] FIG. 1 is a schematic representation of the operation of the global protection device of the present invention;

[0015] FIG. 2 is a schematic geographical representation of how the present global protection system operates around the globe; and

[0016] FIG. 3 is a schematic representation of operation of the present invention in other potentially stolen items, such as cell phones and credit cards.

DETAILED DESCRIPTION OF THE INVENTION

[0017] The present invention, shown in FIG. 1, avoids the disadvantages of prior devices as mentioned above by irreversibly deactivating and/or erasing at least one of the components ~~5,6,7,8 (Figure 1)~~ and/or information within at least one of ~~these~~ the components that are essential for operation of ~~the~~ , for example, a vehicle, so that disassembly or bridging of the components concerned has no effect, since there is no access to the acquisition of functioning replacement parts. These components can include, e.g., the motor electronics 6, the steering column lock 7, the door lock 8, and/or the key 5.

[0018] In order to achieve worldwide protection, the radio signal 9,14 is preferably radiated by a low-orbiting satellite and/or a space station 1, both with high inclination-in order to achieve global coverage. In this case, it is not necessary to fly in a 90° polar orbit, since the transmitter 2 has a certain side width 19 and can cover the inhabited parts of the world already with a 50° inclination because of the rotation of the earth (Figure 2). In the non-covered regions, 17,18, at the poles, this use is of no interest, because there are no consumers there. With today's usual radio density and restrictions on transmitter power, a space station 1 comes into consideration preferably, since they can be kept at a maximum orbiting altitude of up to 400 km for a long period of time, in order to generate the required field strength. Control of the transmitter 2 can take place through radio or another communications medium, e.g., by calling an emergency center 3, which takes over the corresponding activation 20 of the transmitter 2.

[0019] In case of a theft of the vehicle 4, with a key 5 or forced taking of the key 5, the legitimate owner of the vehicle calls a service number by telephone or transmits in some other way information about the theft. After checking his authenticity, e.g., by giving a password in order to prevent malicious deactivation, the identification number of the stolen unit is sent by one or more ground stations 3 to the transmitter 2 in orbit. This identification (ID) number is preferably assigned unambiguously worldwide for every received and/or group of receivers 5,6,7,8, and it can be stored in a database, for example. The transmitter 2 now transmits this ID periodically, preferably worldwide, so that over the course [o] of time the signal 9,14 can be received over the entire face of the earth 16.

[0020] The theft protection within the devices, e.g., the motor electronics 6, steering column 7, or door lock 8 in the vehicle is erased when the indispensable important information in the signal

9 and/or disturbed components is/are recognized by the on-board electronics 6, the key 5, [an/or] and/or the lock 8, without which operation of the vehicle is no longer possible. The receiver [or] 32 of the decoder logic [9] and the safety-relevant components 10 preferably form a unit 21 (e.g., microprocessor with its own internal memory) so that the data traffic 11 of the electronics is "monitored" and can possibly be manipulated, so that deactivation is no longer possible.

[0021] In addition, for deactivation the vehicle 4 can also send signals back to make localization possible more easily; this is not absolutely necessary for protection of the vehicle, however. The system can also be constructed in such a way that only the legitimate owner can trigger this signal, so that an undesired permanent localization of the vehicle is impossible.

[0022] The deactivated components can be later identified as stolen by checking the serial number and/or the disturbed data. For this, a contract workshop can use a corresponding diagnostic device, with which the data from the components 5,6,7,8 can be read. False alarms and intentional deactivations are excluded, and the signal 9,14 can be provided with check sums to permit transmission and/or authenticity errors to be detected.

[0023] For safety reasons, in a vehicle that is moving, a regulated slow disconnection is preferably performed, so that the danger of an accident is avoided. This can occur in such a way that, for example, the vehicle can no longer be accelerated, and a stop is achieved by slowing down gradually. Then the motor can be turned off. In this case, it is irrelevant whether the deactivation takes place immediately or only after a time, after which the theft signal is turned off. For the potential thief, use of such a vehicle is uninteresting, since the vehicle can stop and become unusable after the theft.

[0024] It is also possible to place the receiver [4] 13 not in the vehicle itself, but in the key 5 (distributed security). Modern drive locks preferably use no mechanical locks, but exchange keyed codes 12 between the key and the vehicle, which block the vehicle. In the case of a deactivation by a radio signal 9,14, it is therefore sufficient that at least one of the components 5,6,7,8 contain the turn-off code. At the next attempt to start the vehicle 4, the information through the data exchange 15 spreads ~~preferable~~ preferably through all components, which now deactivate themselves as described above.

[0025] This data exchange can likewise not be stopped, e.g., by involving synthetic information, since signaling takes place in the absence of the correct data 12. These [date] data 12 are generated anew when any contact is made with components 5,6,7,8, and they can only be generated and decoded by them, since the components are identified with each other at the time of manufacture (one-time coding principle).

[0026] A "repair" of the vehicle is thus (preferably) possible thereafter only by exchanging all deactivated components 5,6,7,8 at the same time. A contract workshop can determine at the time the new components are sold, which naturally involves the return of at least one of the deactivated components 5,6,7,8, whether a theft signal 9,14 was responsible for the deactivation or therefore the thief caused the vehicle 4 to stop in attempting to reactivate it. An excuse that the

components were disturbed during an accident and therefore could not be presented cannot be made for the reason that an accident in which all electronic modules 6,7,8 and all keys 5 were disturbed cannot happen. Even surrendering an unauthorized key 5 that has not received a deactivation signal 14 is of no use, since in this case, the read-out of the ID and an identification with the database would inmediately indicate a theft.

[0027] Distributed security also ~~increased~~ increased the reliability of the system, since vehicles are turned off under certain circumstances in areas where receiving the radio signal 9,14 is not always possible (deep garages, etc.) or the receiver is intentionally shielded. It should not happen for the legitimate user that the device is deactivated falsely through bad reception conditions. A receiver 13 integrated into the key holder [is] normally has good reception conditions sufficiently often and one can check regularly that the theft radio ~~service~~ signal 14 is received without errors. If this is not the case, then the receiver in question goes into a metastable state. On the next attempt to start the vehicle, the components check with each other by a comparison 15 of their data, whether at least one of the components was able to receive a signal 9,14 within the permitted time period. If so, then the system is reactivated completely. If not, then the user is signaled that radio contact must be made possible within a certain time period, since otherwise the electronics will be deactivated. If a thief omits this radio contact in a stolen vehicle, then the electronics are likewise deactivated, so that in this case the vehicle 4 remains useless to the thief.

[0028] Since [the] a receiver can be greatly miniaturized, this system is also very well suited for devices that must make radio contact in any case, such as, e.g., radio telephones [21] 31 (Figure 3). The receiver in this case can be included in the chip card 22 and/or the telephone [21] 31. If one of the devices receives a deactivation signal 23,24, at the time of the next use, when the card 22 must be inserted into the telephone [21] 31, the chip card 22 is deactivated by the data exchange 26 between the components, whereby the telephone can still send out signals 25 even after a deactivation, so that localization is possible.

[0029] In principle, the receiver can also be built into the newest generation of check cards 27, so that here a protection of E.C. cards, credit cards, and telephone cards becomes possible. A card that receives a deactivation signal, 28, 29 (this can also derive from the automatic device 30 itself) can detect ~~likewise~~ and likewise erase its internal memory. At the next attempt to use the card, a money device 30 can detect this and take corresponding further steps, e.g. recording the person on video, reporting the site to the motion detector, locking the doors, etc.

~~(Safety Device for Overall Protection of Objects with Electronic Components)~~
~~Patent claims~~

CLAIMS

What is claimed is:

~~(Safety Device for Overall Protection of Objects with Electronic Components)~~

~~Summary~~

ABSTRACT OF THE DISCLOSURE

[[1]] The invention concerns a device and a procedure for global protection of objects with electronic components.

[[2.1]] An electronic theft protection device can be circumvented by shielding, exchanging, or bridging critical components. The new invention avoids this by making the protection a functional component of the object to be protected.

[[2.2]] The security ~~device~~ devices , e.g., in a vehicle, become active by at least one of the components ~~5,6,7,8 (Figure 1) and or~~ and/or information within at least one component that is essential for operation of the vehicle is deactivated irreversibly and or erased, so that even a disassembly or bridging of the component concerned can achieve no effect, since acquisition of a functional replacement part is not available. The components can, for example, be placed in the motor electronics [6], the steering column lock [7], the door lock [8], and/or the key [5].

[[2.3]] Through miniaturization of the receiver, any electronic devices can be protected. This includes, among other things, radio telephones [("Handies")], (Euro-)checkcards and cash cards, credit cards, telephone cards, keys to electronic systems, mobile electronic devices, such as cassette recorder, CD players, clocks, computers, etc.